拒絶理由通知書

特許出願の番号	平成１１年　特許願　第０５９０４９号
起案日	平成１５年　９月　１日
特許庁審査官	青木　重徳　　４２２９　５Ｍ００
特許出願人代理人	河野　登夫　様
適用条文	第２９条柱書、第２９条第２項、第３６条

15.11.-7

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

【Ａ】この出願の下記の請求項に係る発明は、下記の点で特許法第２９条第１項柱書に規定する要件を満たしていないので、特許を受けることができない。

記

・請　求　項：１
・備　　考

計算法、作図法と認められる発明は、一般に人間の推理力や記憶力を利用するものであって自然法則利用の技術的手段を伴うものでないから、特許法第２条に定義されている発明とは認められず、同法第２９条の特許要件を備えていないと解するのが原則である。

そして、本願請求項１に係る発明は、本願明細書及び図面に記載されている事項を参酌すると、分割特定情報から計算により秘密鍵を生成する方法が記載されており、その間何らの装置も用いていないことから、上記原則が適用できる。

・請　求　項：２
・備　　考

文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、たとえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。

そして、本願請求項２に係る発明では、分割した分割特定情報を利用して生成した秘密鍵に基づき、通信相手の分割特定情報に対応する成分から共通鍵を生成し、該共通鍵を使って暗号を作成する方法について記載しており、その間何らの

装置も用いていないことから、上記原則を適用できる。

・請　求　項：３
・備　　考
文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、たとえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、これを暗号による通信方法と解しても暗号による思想表現の方法と認められ、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。

そして、本願請求項３に係る発明では、分割した分割特定情報を利用して生成した秘密鍵に基づき、通信相手の分割特定情報に対応する成分から共通鍵を生成し、該共通鍵を使って暗号を作成して通信を行う方法について記載しており、その間何らの装置も用いていないことから、上記原則を適用できる。

【Ｂ】この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第２号に規定する要件を満たしていない。

記

本願請求項１－３に係る発明では、「第１ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として前記秘密鍵を生成する」旨が記載されているが、「複層構造」や「単層構造」が秘密鍵の何を意味しているのか、本願明細書や図面に記載されている事項を参酌しても意味不明である。

従来技術の第【０００８】段落には「この結託問題の難しさは、ＩＤ情報に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。」旨が記載されており、前記「複層構造」がセンタ秘密と個人秘密との二重構造のことを意味するものかとも考えられるが、該構成に対応する「単層構造」が何なのかが明細書には記載されていない。

よって、請求項１－３に係る発明は明確でない。

【Ｃ】この出願の下記の請求項に係る発明は、その出願前日本国内において頒布された下記の刊行物に記載された発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）
・請　求　項：１－３
・引用文献等：１

・備　　考

請求項１－３に係る発明の「複層構造」や「単層構造」が何を意味するものか不明であるものの、引用文献１には、ＩＤベクトルの分割によりエンティティ固有の秘密鍵を生成し、該秘密鍵と通信相手エンティティのＩＤベクトルに基づいて生成した共通鍵を使って暗号通信を可能とする方法が記載されている。

そして、引用文献１に記載されているものは、エンティティと特定情報を複数ブロックに分割して利用する点において、本願請求項１－３に係る発明と本質的に同様な方法を記載したものである。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

引　用　文　献　等　一　覧

１.辻井重男，村上恭通，笠原正雄，“第四の鍵共有方式－拡張ＩＤ－ＮＩＫＳの提案”，１９９９年暗号と情報セキュリティシンポジウム予稿集，日本，１９９９年　１月２６日，Volume 1 of 2，ｐ．１３５－１４０

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ第７版
　Ｈ０４Ｌ９／０８

・先行技術文献
　笠原正雄，村上恭通，辻井重男：“３層構造を有する鍵共有方式の提案”，電子情報通信学会技術研究報告，１９９９．５．２０発行，Ｖｏｌ．９９，Ｎｏ．５７（ＩＳＥＣ９９－２），ｐ．９－１３

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。